NORTH DAKOTA

HOMELAND SECURITY

ANIT-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

(Montana; North Dakota) **Fort Peck Dam releases to rise to 55,000 cfs Friday.** On June 7, the same day that the U.S. Army Corps of Engineers bumped the releases from Fort Peck Dam in Fort Peck, Montana up to a new historic high of 50,000 cubic feet per second (cfs), the agency said it would add an extra 5,000 cfs by June 10. Continued high runoff into the reservoir, prompted the change. "Inflows into Fort Peck have been averaging above forecasted levels while inflows to the Garrison reservoir have been averaging a little below forecasted levels," the chief of the Missouri River Water Management office said. Garrison in central North Dakota is the next dam downstream. "As a result, releases at Fort Peck will be increased to better balance the remaining storage between Fort Peck and Garrison." Peak releases are expected to continue into August. It is not yet known what the additional increase will do to communities downstream of the dam. Source: http://billingsgazette.com/news/state-and-regional/montana/article_c0df41b6-fdcd-5ee8-a084-a1c71ff54843.html

Spillway gates at Garrison Dam back in business Monday. The emergency repairs to the Garrison Dam spillway in North Dakota were successful, and the spillway gates were back in business early June 6. The U.S. Army Corps of Engineers raised 19 gates to release 20,000 cubic feet per second (cfs) of water, after a contractor patched up a pothole that formed when the gates were raised to pass floodwater for the first time in the dam's 57-year history June 1. Barring any other issues, the gates will stay open, and all 28 of them should be in use by the week of June 13, raised slightly higher to increase the flow rate. The gates will contribute about 65,000 cfs to the full release of 150,000 cfs scheduled to start sometime the week of June 13. Meantime, the Corps expects the lake behind the dam will continue to rise to 1,856 feet elevation. The new record elevation will occur because the top of the spillway is higher when the gates go up, and because of the bulge of water expected from mountain snowmelt. Source: http://www.bismarcktribune.com/news/state-and-regional/article_dcaf0128-908c-11e0-aafd-001cc4c03286.html

Amtrak's Empire Builder curbed by freight backlog. Amtrak said a backlog of freight caused by flooding along rail lines in Montana and North Dakota is disrupting passenger rail service from Minnesota to the Pacific Northwest. The Amtrak spokesman said the railroad's Empire Builder line between St. Paul, Minnesota, and Spokane, Washington, will remain closed though June 7. The railroad announced June 1 that it canceled service due to flooding. Amtrak's spokesman said the railroad is waiting for the backlog of freight to clear so that there will be no delays in passenger traffic. Source: http://billingsgazette.com/news/state-and-regional/montana/article_1347e872-9082-11e0-96ba-001cc4c002e0.html

Backup levee built to protect SD town; planned evacuation of Bismarck neighborhoods delayed. The U.S. Army Corps of Engineers began construction of a backup levee June 5 to protect Dakota Dunes, South Dakota from the fast-rising Missouri River. A Corps engineer said the 1.4-mile long secondary levee is slated to be completed by June 9. The earthen dike is being placed as insurance against increased releases at Gavin's Point Dam upstream from Dakota Dunes, he said. The Missouri River was expected to rise about 8 feet to 1,098 feet above sea

level by June 14 in the city of about 2,500 people, some of whom have evacuated ahead of the planned crest. Officials said construction of the primary levee is still under way to protect the city 2 feet beyond the projected high level. Source: http://www.inforum.com/event/article/id/322400/group/homepage/

Repairs at Garrison Dam. Repairs to the Garrison Dam`s Spillway slab were expected to be completed late June 5. Spillway gates at the Garrison Dam were used for the first time June 1. Early June 4, they were closed. "When we utilize the spillway, we like to see a nice, uniform flow ...and when we opened-up the gates, initially, we saw irregularities," said a U.S. Army Corps of Engineers spokesman. "There was one area where the water was spraying up above the linear flows and that raised a concern for us, that something was not right with the slab. So we shut down the flows and looked at it and there were concrete sprawls, which people have equated to a pothole ... We decided we needed to determine whether those were going to continue to progress or if we should fix them," he continued. "What we are seeing ...are very minor surface issues ... but because of the large aggregate used in the concrete, we are seeing some of those surfaces sprawl. What we saw at the end of the spillway was a large scale of this occurring ... and we decided to chip those out, remove the loosened concrete and go back in with a new concrete material," the spokesman noted. That material sets within an hour and the spillway gates were expected to re-open June 6, giving it time to cure. Officials said they are not concerned about the dam's structural integrity. Source: http://www.kfyrtv.com/News_Stories.asp?news=49693

REGIONAL

(Montana) **Fort Peck spillway releasing record amounts.** In Eastern Montana, northwest of Billings, the Fort Peck Spillway is letting out record amounts of water and engineers are set to increase that two more times by June 7 to a full total of 50,000 cubic feet of water per second. The U.S. Army Corps of Engineers said the dam can not handle the high amounts of water expected in the next few days, so they must release as much as they can now. The Corps already has been meeting with people living in all points west, mainly in Poplar and Wolf Point, getting them ready for potential low lying flooding. Source: http://www.nbcmontana.com/news/28139397/detail.html

(Montana) **Contaminated Fort Peck area cut off from water.** A pipeline failure has cut off the water supply to about two dozen homes in a contaminated area of the Fort Peck Indian Reservation in Montana, leaving residents without drinking and bath water for more than 3 weeks. The pipeline from Poplar's water supply system to the homes north of the city has been out of service since May 13, said the Fort Peck Assiniboine and Sioux Tribes' environmental program manager. The 23 homes have received the piped water since 2005, after the U.S. Environmental Protection Agency (EPA) ordered three oil companies to build the line because of a spreading underground plume of contamination from the East Poplar oil field. The water pipeline has had dozens of breaks since Murphy Exploration and Production Co., Pioneer Natural Resources USA Inc., and Samson Hydrocarbons Co. built it, the program manager said.

The tribes believe the problems are due to poor installation and operation, and that the oil companies should be forced to provide them with a reliable system. The EPA is working with state officials to determine whether the line was improperly constructed or if there is another reason for the failure, an EPA spokeswoman said. Meanwhile, the companies are providing bottled water to the homes. Source: http://www.mysanantonio.com/news/article/Contaminated-Fort-Peck-area-cut-off-from-water-1410390.php

(South Dakota) **7,000 South Dakotans wait as water tests levees.** Officials expressed hope June 7 that most houses in Dakota Dunes, South Dakota will be safe from Missouri River flooding, but homeowners in other nearby upstream neighborhoods might not be so fortunate. "We'll still have houses that most likely will be flooded," a policy adviser in the governor's office sad. "There are still people who will lose basically all their possessions." The issue was of great concern June 7 as construction workers hauled in dirt to build earthen levees to stay ahead of the rising river. About 180 truck crews were at work dumping dirt at a rate of one load every 45 seconds. Missouri River flooding has forced about 7,000 South Dakotans from their homes. About half of them are in Dakota Dunes in the state's southeast corner. June 7 was another day of residents, volunteers, and construction crews teaming to protect riverside lands in southeast and middle parts of the state. Dakota Dunes, Pierre, and Fort Pierre are the three cities most at risk, because of their low topography, as the Missouri moves through South Dakota swollen with snowmelt and spring rain from points northwest. Source: http://www.argusleader.com/article/20110608/NEWS/106080323/7-000-South-Dakotans-wait-water-tests-levees?odyssey=nav|head

National

Nothing Significant to Report

International

2 new E. coli deaths as EU holds emergency meeting. Germany reported two more deaths and 300 more E. coli cases June 8, but its health minister insisted that new infections were dropping, giving some hope that the world's deadliest E. coli outbreak was abating. The European Union is getting concerned about Germany's handling of the crisis. The death toll has risen to 26 — 25 in Germany plus one in Sweden. Germany's national disease control center, the Robert Koch Institute, said the number of reported cases in Germany rose by more than 300 to 2,648. Nearly 700 of those affected are hospitalized with a serious complication that can cause kidney failure. Another 100 E. coli cases are in other European countries, and the United States. The Koch Institute said there was a declining trend in new cases, but added it is not clear yet whether that is because the outbreak is truly waning or whether it is because consumers are staying away from the raw vegetables believed to be the source of the E. coli. Weeks after

the outbreak began May 2, German officials are still looking for its cause. Spanish cucumbers were initially blamed, then ruled out after tests showed they had a different strain of E. coli. Investigators June 5 pointed the finger at German sprouts, backtracking a day later when initial tests were negative. The German health minister reiterated that the source of the infection may never be found, a stance U.S. experts have called a cop-out. A warning against eating cucumbers, tomatoes, lettuce, and vegetable sprouts is still in place. Source: http://www.boston.com/lifestyle/health/articles/2011/06/08/germany_rise_in_reported_ecoli_cases/

Greenpeace activists delay Dutch nuclear waste train. A train carrying nuclear waste from the Borssele nuclear power plant in Netherlands to a reprocessing facility in Normandy, France, was delayed by almost 3 hours June 7 after dozens of Dutch Greenpeace activists attempted to block the train by chaining themselves to the rail track. Police said the train resumed its journey and crossed over the border into Belgium after they arrested and removed some 33 activists attempting to block the train from leaving Borssele in the Dutch province of Zeeland. While most of the activists who had chained themselves to the tracks were removed by cutting the chains using saws, in some cases police were forced to use blow torches to free them. The activists were released from police custody after the train's departure. They have been served with summons to appear in court and are expected to be charged later with disturbing public order or hindering a train. Although similar protests were planned at the Belgian border town of Essen also, the move was foiled by heavy security presence. Source: http://www.rttnews.com/Content/MarketSensitiveNews.aspx?Id=1641218&SM=1

Banking and Finance Industry

Citigroup breach exposed data on 210,000 customers. Citigroup admitted June 8 that an attack on its Web site allowed hackers to view customers' names, account numbers and contact information such as e-mail addresses for about 210,000 of its cardholders. Citigroup did not say how the Web site, Citi Account Online was compromised. The bank discovered the breach early in May. Other customer information, such as Social Security numbers, birthdates, card expiration dates, and the three-digit code on the back of the card, were not exposed, the company said. The affected customers are being contacted by Citigroup. Although hackers may have not gained complete information on cardholders, the contact information is enough for scammers to try and elicit more information through targeted attacks. Source: http://www.pcworld.com/businesscenter/article/229868/citigroup_breach_exposed_data_on_210000_customers.html

FBI releases bank crime statistics for first quarter of 2011. During the first quarter of 2011, there were 1,092 reported violations of the Federal Bank Robbery and Incidental Crimes Statue, a decrease from the 1,183 reported violations in the same quarter of 2010. According to statistics released June 6 by the FBI, there were 1,081 robberies, 9 burglaries, 2 larcenies, and 1 extortion of financial institutions reported between January 1, 2011 and March 31, 2011.

Source: http://www.fbi.gov/news/pressrel/press-releases/fbi-releases-bank-crime-statistics-for-first-quarter-of-2011

Foreclosure fraud price tag: $20 billion. The nation's largest mortgage companies are operating on the assumption that they will have to pay as much as $20 billion to resolve claims of widespread foreclosure abuse, an amount four times what they had originally proposed, the top federal official overseeing the discussions told state officials June 6, according to people who participated in the conversation. The associate U.S. Attorney General (AG) told a bipartisan group of state attorneys general during a conference call that he believes the banks have accepted the realization that a wide-ranging settlement to the months-long probes will cost them much more than the $5 billion offer they floated in May, according to officials with direct knowledge of the call. The assistant AG said he is basing his belief on his recent conversations with representatives of the five targeted firms: Bank of America, JPMorgan Chase, Wells Fargo, Citigroup, and Ally Financial. Source: http://www.huffingtonpost.com/2011/06/06/foreclosure-fraud-20-billion_n_872207.html

AFP assisting in $540 million U.S. bank fraud case: report. The Australian federal police are assisting the United States in an alleged bank fraud case where online poker sites may have laundered $540 million via an Australian payments processor, according to Fairfax Media. The FBI alleges that Intabill, registered in the British Virgin Islands, processed a minimum of $543,210,092 worth of transactions for the poker companies Full Tilt, PokerStars, and Absolute Poker between mid-2007 and March 2009. Source: http://www.businessspectator.com.au/bs.nsf/Article/AFP-assisting-in-US540-million-US-bank-fraud-case--pd20110604-HH27T?OpenDocument&src=hp3

Chemical and Hazardous Materials Sector

NRC inspection results for operating nuclear power plants in the US released. The Nuclear Regulatory Commission (NRC) June 6 issued inspection results for the 104 operating U.S. nuclear power reactors, regarding their guidelines for continuing to protect the public even if accidents were to damage reactor cores. The NRC carried out the Severe Accident Management Guideline (SAMG) inspections at the request of the agency task force reviewing the lessons to be learned from the March 11 earthquake and tsunami in Japan, and the resulting damage to the Fukushima Dai-ichi nuclear power plant. The resident inspectors examined where plants keep SAMGs, how the guidelines are updated, and how plants train personnel to carry out the guidelines. Inspectors found that all plants have implemented the guidelines, with 97 percent keeping SAMG documents in their Technical Support Center, generally considered the best location for properly implementing the guidelines. The inspectors found SAMGs in 89 percent of plant control rooms, and in 71 percent of plant Emergency Operations Facilities. Only 42 percent of the plants, however, presently include SAMGs in their periodic review/revision procedures. The inspectors found tjat staff at 92 percent of plants received initial training on SAMGs. When examining how the plants exercise carrying out SAMGs, inspectors found only 61 percent periodically include the guidelines in their emergency drills. Source:

http://www.pennenergy.com/index/power/display/4468425574/articles/pennenergy/power/nuclear/2011/june/nrc-issues_inspection.html

Commercial Facilities

(Michigan) **Police apprehend man sought in Trenton bomb threats.** The Trenton, Michigan, Police Department and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) have a person of interest in custody in connection to bomb threats made in April, the mayor of the Michigan town said June 7. The man is believed to have been involved with an April 28 bomb threat at Trenton High School, a suspicious device that was found at the high school, and an explosive device that was detonated at ACO Hardware. The man's home in Deerfield Estates in Flat Rock was being searched by federal agents from the ATF. Flat Rock police, and the Downriver SWAT Team are assisting in the investigation. Source: http://trenton.patch.com/articles/atf-police-apprehend-man-sought-in-bomb-threats

(Michigan) **ATF seeks Trenton explosives suspect.** The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) is searching for a man it said is responsible for a bomb threat at Trenton High School and another explosion in Trenton, Michigan, WDIV 4 Detroit reported June 6. The bureau said a man called in a bomb threat April 28 at the high school. An explosive device was found in the school's teachers' parking lot, the ATF said. A bomb squad "rendered the device safe," the ATF said. The same man is suspected of detonating a home-made explosive device April 29 near the ACO Hardware store at 3080 Van Horn Rd. The bureau said it is offering a $5,000 reward to anyone with information leading to an arrest. The Trenton Police Department, the ATF, and the Michigan State Police are all involved in the investigation. Source: http://www.clickondetroit.com/news/28147039/detail.html

(Ohio) **2 suspected of having material to make bomb.** At least two juveniles were being investigated June 6 for having bomb-making equipment inside a garage in Sylvania Township, Ohio. Officers June 4 found gunpowder, powder scraped from sparklers, and other "odds and ends that normally you don't find or see" inside the garage, a police lieutenant said. Authorities were initially investigating a criminal damaging complaint and had taken two boys into custody when one of the boys said another was trying to make bombs and planned to plant them at another juvenile's home and at Wal-mart, according to a Toledo police incident report. Sylvania Township police went to the boy's home, looked in the windows of an unattached garage, and saw the possible "bomb-making equipment," authorities said. The Toledo bomb squad was called in to remove and secure the materials, police said. Source: http://www.toledoblade.com/Police-Fire/2011/06/07/2-suspected-of-having-material-to-make-bomb.html

(Colorado) **Fort Collins bomb squad destroys suspicious package found at shopping center.** Fort Collins, Colorado police said they are still trying to determine the contents of a suspicious package found June 5 at a Fort Collins shopping center. The Fort Collins Coloradoan said police used a water cannon to destroy the device. The package was found near a beauty parlor at

Front Range Village by a groundskeeper. Police cordoned off the parking lot, and the bomb squad used a robot with a camera and X-ray to inspect the device. The device was described as a small box with wires sticking out, and a fuse. Source: http://www.therepublic.com/view/story/50427a878fdf429dbe8949b7f31c10ad/CO--Package-Destroyed/

Communications Sector

Skype hangs up on users yet again. Users around the world again experienced problems using Skype June 7. With seemingly identical problems in May, punters initially experienced frustration signing into the service before later reporting that the VoIP software had crashed on their machine. Skype played down the scope of the problem, which it blamed on a ""configuration problem," in an update to its status page. It promised to resolve the snafu via an automatic update that would be in place within an hour or so. The symptoms of the latest glitch, at least, are identical to problems experienced across the VoIP network less than 2 weeks ago. Resolving the problem then involved deleting a file called "shared.xml" on users' machines that had somehow been corrupted. Source: http://www.theregister.co.uk/2011/06/07/skype_outage/

Docomo network glitch hits 1.72M users. Japanese mobile market leader NTT Docomo said June 6 a mysterious network glitch was affecting up to 1.72 million mobile customers, making it difficult for them to make calls or send messages. According to a Dow Jones Newswires report, the fault was first registered the morning of June 6 Japanese time) in the greater Kanto region, which includes Tokyo. A Docomo spokesman said trouble at a facility that processes phone number information likely led to network connection problems, and that these problems caused people to make repeated attempts to call or send messages, exacerbating the situation by increasing the burden on base stations. Eight hours after the problem was flagged, the operator said on its Web site the situation was gradually improving. However, the spokesman said the firm was not sure when the situation would return to normal. The 1.72 million subscribers thought to be affected by the problem represent almost 3 percent of Docomo's 58 million mobile customer base. Source: http://www.mobilebusinessbriefing.com/article/docomo-network-glitch-hits-1-72m-users

Critical Manufacturing

Nothing Significant to Report

Defense/ Industry Base Sector

Boeing says under 'continuous' cyber attack. U.S. aerospace giant Boeing is under "continuous" cyber attack but there has been no breach of its databases, the chief executive of Boeing Defense, Space and Security said June 3. "We, as are other global enterprises, are under a continuous state of cyber attack and cyber probing," he said. "We recognize the reality of global business today, is that cyber attacks are part of business and we've been prepared for that so this is not a surprising environment to us," he told a media briefing in Singapore. He did not want to mention how often the attacks took place or the people behind it but said Boeing's investment to protect its systems from hackers has paid off. "I can tell you that the defensive capabilities that we've built up are very effective, and give us confidence and our enterprise is secure because of that investment," he said. Source: http://news.yahoo.com/s/afp/20110603/tc_afp/aviationboeinginternettechnologysecurity_20110603063716

Stolen RSA data used to hack defense contractor. Defense contractor Lockheed Martin has confirmed that a recent attack on its network was aided by the theft of confidential data relating to RSA SecurID tokens employees use to access sensitive corporate and government computer systems. According to an e-mail the company sent to reporters, theft of the data for the RSA tokens was "a direct contributing factor" in May's intrusion into its network. New York Times, which reported on the e-mail earlier, cited government and industry officials, who said the hackers used some of the purloined information and other techniques to "piece together the coded password of a Lockheed contractor who had access to Lockheed's system." Lockheed said it detected the attack soon enough to prevent those responsible from accessing important data. The company is in the process of replacing 45,000 SecurID tokens used by its workers when logging in corporate networks from outside the office. The contractor, which makes fighter planes, spy satellites, and other gear related to national security, is also requiring workers to change their passwords. Source: http://www.theregister.co.uk/2011/06/06/lockheed_martin_securid_hack/

Emergency Services

(Texas) **Cop accused of lying about citizenship to join FBI.** A Fair Oaks Ranch, Texas police officer who wanted to join the FBI has been charged with lying about his citizenship to get a job there. The FBI Joint Terrorism Task Force (JTTF) opened a full-blown investigation last year of the 30-year-old, for his "aggressiveness" in wanting to join the FBI, and his e-mailed request to the agency seeking to attend weapons of mass destruction training being taught by the JTTF, according to a criminal complaint affidavit unsealed June 6. The Iranian-born officer, now a U.S. citizen, was taken to federal court in San Antonio June 3 on a charge of making false statements about his citizenship to get a job in law enforcement. He was released on $50,000 unsecured bond following a hearing before a U.S. magistrate judge. If convicted, he could face up to 5

years in prison. Source: http://www.beaumontenterprise.com/news/article/Cop-accused-of-lying-about-citizenship-to-join-FBI-1413462.php

Popular police cars Crown Victorias prone to explode, tied to deaths. The last minutes of a Florida state police trooper's short life were spent in a Crown Victoria Police Interceptor — a car praised for its strength, hailed for its durability and known to explode in high-speed rear-end crashes. By one estimate, fiery Ford Crown Victoria crashes have claimed more lives than the notorious Ford Pinto, subject of a nationwide recall in 1978. An officer, who died last year, is the latest of at least 30 law enforcement officers since 1983 who died in such accidents. Five were in Florida. Another 20 escaped patrol cars that crashed and caught fire. Ford knew there could be issues with the position of the car's fuel tank as early as the 1960s, documents obtained by the Palm Beach Post show. Sales continue even though there is evidence Ford's widely touted safety system, an anti-fire device introduced in 2005, is useless in the worst fires: the fire suppressant was tested on a nearly empty gas tank. In two fatalities, including the most recent officer's crash, the system failed to extinguish the fire. And there are still hundreds of Crown Victorias on local roads with no anti-fire device at all. Of 1,714 Crown Victorias in use by sheriff's deputies and police officers in the south Florida region's six largest cities, just five are equipped with Ford's fire suppressant system. Source: http://www.palmbeachpost.com/news/popular-police-cars-crown-victorias-prone-to-explode-1520076.html?viewAsSinglePage=true

(New York) **World Trade Center memorial worksite may be guarded by 600 police officers.** New York plans to deploy more than 200 police officers at the World Trade Center site in Manhattan by mid-July who will focus on security for the opening of a memorial to victims of the September 11 attacks, the police commissioner said. The amount of personnel will be increased "incrementally" as construction continues at the site and buildings are opened, and more than 600 officers may eventually be based in a command unit there, he told reporters following a counterterrorism conference at police headquarters June 6. There are no specific threats against the city, although New York must be concerned about possible revenge attacks in the wake of the killing of al-Qaida leader in Pakistan May 1, the commissioner said. Source: http://www.bloomberg.com/news/2011-06-06/wtc-memorial-worksite-may-be-guarded-by-600-new-york-city-police-officers.html

LulzSec claims it hacked FBI linked organization. Hacking group Lulz Security claimed it had hacked and defaced the Web site of the Atlanta, Georgia chapter of InfraGard, an organization affiliated to the FBI, and leaked its user base. The group said they hacked the InfraGard site after the North Atlantic Treaty Organization and the U.S. President had raised the stakes with regard to hacking, by treating it as an act of war. The Web site of InfraGard's Atlanta chapter was not accessible late June 5 and returned the message that the site was "under construction" as the future home for the Atlanta InfraGard Member's Alliance. A cache of the site on Google search confirmed the site was that of InfraGard Atlanta. InfraGard describes itself an association of businesses, academic institutions, state, and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. LulzSec claimed to have obtained about 180 logins from the hack of

the InfraGard Atlanta web site, and all of them were affiliated to the FBI in some way. It also claimed to have obtained the login of Karim Hijazi, CEO of Unveillance, a network security company in Delaware. Source: http://www.computerworld.com/s/article/9217320/LulzSec_claims_it_hacked_FBI_linked_organization

(Texas) **Detectives seek motive in killing of Texas deputy.** Detectives continue to seek clues to the motive behind the ambush-style slaying of a Bexar County sheriff's deputy at a San Antonio, Texas, intersection. Federal and local officials arrested the suspect at his family's double-wide mobile home 15 miles south of San Antonio around 4 p.m. June 5, after FBI agents swarmed the property and ordered him and his wife to exit the home, according to a sheriff's office statement. His wife also was taken into custody for questioning and their child was placed with relatives, the statement said. Authorities said a truck matching the description of the suspect vehicle was found registered to the suspect at a San Antonio body shop. Investigators suspect an automatic weapon found at the home fired the deadly shot, according to the sheriff's office statement. Investigators had said shortly after the May 28 slaying that they did not believe the deputy was specifically targeted, but that the killer may have been looking for a law enforcement officer to kill. Authorities had not established a motive as of the night of June 5. Source: http://abclocal.go.com/ktrk/story?section=news/state&id=8172398

ENERGY

EPA faults State Department review of TransCanada pipeline. The U.S. State Department failed to properly analyze potential environmental impacts of TransCanada Corp.'s planned pipeline to carry crude from Canada to the Gulf Coast, according to the Environmental Protection Agency (EPA). The department's review of the $7 billion project lacks information the EPA needs to assess effects on groundwater or air pollution, according to a letter sent to the assistant secretary for economic, energy and business affairs. The State Department is reviewing the project because it crosses an international boundary. Environmental groups and some Democrats oppose the planned 700,000-barrel-a-day pipeline, which would carry crude from Canada's oil sands across Montana, South Dakota, Nebraska, Oklahoma, and Texas to U.S. refineries. The EPA has said a decision will be issued by the end of this year. The agency raised concerns last year about the project after the State Department released a preliminary environmental review. It said more work was needed on potential greenhouse-gas emissions from the project, pipeline safety, and impacts on wetlands and migratory birds. Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2011/06/07/bloomberg1376-LMFOUM0UQVI901-0PKOBAUPO4KJI5I8L0MIK4P8P3.DTL

(Arizona; Texas; New Mexico) **Ariz. fire threatens 40% of El Paso's power.** El Paso Electric Co., supplier of power to an oil refinery and the U.S. Army's Fort Bliss, said it is seeking alternative power supplies should an Arizona wildfire cut electrical lines from Palo Verde, the nation's largest nuclear generating plant located in Wintersburg, Arizona. The Wallow Fire is on track to reach within 3 days high-voltage links that deliver 40 percent of the power used by 371,000

homes and businesses in western Texas and southeastern New Mexico, including the 1,700-square-mile Fort Bliss base, a spokeswoman for the El Paso, Texas-based utility owner said June 8. The blaze, which started May 29, has scorched an area 21 times larger than Manhattan. The utility warned June 7 it would begin cutting power temporarily to parts of its service area as a "last resort" to avoid a wider blackout. Residents of Springerville, Arizona, near El Paso's lines, have been urged to prepare for evacuation by the sheriff of Apache County, according to the Web site of the incident command for the fire. None of the fire is contained, the June 8 report said. Fire damage to the lines from Palo Verde in Arizona may knock out 633 megawatts of supply, the utility owner said June 7. That is enough for about a half million average U.S. homes, according to statistics from the Energy Department in Washington. The Wallow Fire has raged over 311,491 acres south and west of Alpine, Arizona. The fire has destroyed 10 structures and damaged one. The Apache County Sheriff's Office has ordered evacuation of at least four towns. The fire has not yet interrupted the power grid, a spokeswoman for the Western Electricity Coordinating Council said June 8. Source: http://www.bloomberg.com/news/2011-06-08/arizona-fire-threatens-40-of-el-paso-electric-s-supply-as-lines-in-path.html

TransCanada reopens Keystone oil pipeline. There were no concerns about the integrity of the 1,300-mile Keystone oil pipeline following a May 29 spill in Kansas, the U.S. government said. Canadian pipeline company TransCanada restarted the Keystone oil pipeline during the weekend of June 4 and 5. The Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) issued a corrective action prohibiting a restart the week of May 30 but reconsidered in time for a June 5 restart. Source: http://www.upi.com/Business_News/Energy-Resources/2011/06/06/TransCanada-reopens-Keystone-oil-pipeline/UPI-85081307364816/

Food and Agriculture

(Tennessee; Virginia) **E. coli sickens 8 in Tenn., kills 2-year-old in Va.** A 2-year-old girl from Dryden, Virginia, died June 5 from an E. coli bacterial infection that also sickened another person in close contact with her, and East Tennessee hospitals have reported at least eight other E. coli infections since June 1. The medical director of the Northeast Regional Health Office in Johnson City, Tennessee, said seven of the cases were from the same strain of bacteria, but a common cause has not been found, according to The Knoxville News Sentinel. The director said some of the patients ate improperly cooked meat, but others were infected while swimming in untreated water. The department is treating the cases as an outbreak and interviewing people who became ill from E. coli to learn the likely causes of infection. A Virginia Department of Health spokesman told the Bristol Herald-Courier that lab results confirmed the presence of E. coli in the 2-year-old child who died. According to a coroner's report, the source of exposure was believed to be a contaminated pool. Source: http://www.foxnews.com/health/2011/06/07/e-coli-sickens-8-in-tenn-kills-2-year-old-in-va/

FDA data prompts Pfizer to suspend poultry drug. A commonly used animal drug is being suspended from sale in response to new U.S. Food and Drug Administration (FDA) data showing it increases arsenic levels in chicken livers. Though public health and industry experts stress that the levels of arsenic found in the new FDA study were very low, and that eating poultry treated with the drug, known as Roxarsone, "does not pose a health risk," Alpharma, a subsidiary of drug giant Pfizer, said June 8 it is voluntarily halting the sale of the drug, which has been used by poultry producers to promote growth and combat parasites since the 1940s. Roxarsone, which contains arsenic, a known carcinogen, is also approved for use in swine and turkey production and is known to improve coloration in meat products. FDA officials told reporters June 8 that the move to halt the sale of the drug is aimed at reducing unnecessary exposure, not out of immediate concern over human health impact. Source: http://www.foodsafetynews.com/2011/06/new-fda-data-prompts-pfizer-to-suspend-poultry-drug/

Salmonella cases rise in United States, federal report shows. Food poisoning cases caused by salmonella have increased by 10 percent in recent years, despite widespread campaigns to educate consumers and foodmakers about food preparation and handling, according to new federal statistics that detail the stubborn presence of salmonella in the U.S. food supply. The findings are part of an annual food safety report card released by the U.S. Centers for Disease Control and Prevention (CDC), which since 1996 has tracked the prevalence of the nine most common food-borne pathogens. About one in six Americans gets sick from food poisoning every year, and 3,000 die, the government said. The data, which are extrapolated nationally based on illnesses reported in 10 states, show a decline in illnesses from E. coli O157:H7, one of the most deadly food-borne bacteria in this country. From 1997 to 2010, the number of E. coli O157:H7 infections dropped by half, according to the CDC. Federal health officials credit more stringent federal regulation, better detection and investigation of E. coli O157:H7 outbreaks, and steps taken by the food industry, particularly beef processors, to prevent contamination at slaughterhouses. Officials also say food workers and consumers have become better educated about the safe handling and cooking of meat. Source: http://www.washingtonpost.com/politics/salmonella-cases-rise-in-united-states-federal-report-shows/2011/06/07/AGxNbHLH_story.html

(Washington) **Deadly horse virus contained, Department of Agriculture says.** It appears the recent outbreak of the neurological form of Equine Herpes Virus 1 has been contained, the Washington State Department of Agriculture said. Concern about this potentially fatal disease of horses caused many organizers to cancel long-planned horse shows, rodeos, trail rides, and parades. Eight horses in Washington State were infected. Four were among the 34 horses from Washington at a National Cutting Horse Association event in May in Ogden, Utah, where the disease apparently spread. The state veterinarian believes sufficient time has elapsed for signs of nEHV-1 to appear in horses exposed at the National Cutting Horse Association Western National Championships, as well as their stable and pasture mates. Horse owners may lift the quarantine on positive or exposed animals 21 days after the end of symptoms if they receive laboratory confirmation that the animal is no longer contagious. Source:

http://www.king5.com/news/local/State-vet-recommends-easing-of-horse-movement-restrictions-123123988.html

SimplyThick: Public health notification - Risk of life-threatening bowel condition. Simply Thick, LLC June 4 announced a voluntary recall of its SimplyThick thickening gel products manufactured at a food processing plant owned and operated by Thermo Pac, LLC. This voluntary recall is limited to only those products manufactured at the Stone Mountain, Georgia plant. The SimplyThick thickening gel products are being recalled because the U.S. Food and Drug Administration (FDA) advised the company that Thermo Pac, LLC failed to file with the FDA a scheduled process designed to ensure that vegetative cells (harmful bacteria) of possible public health significance are destroyed during the manufacturing process. The FDA notified parents, caregivers and health care providers not to feed SimplyThick, a thickening agent for management of swallowing disorders, to infants born before 37 weeks gestation. The product may cause necrotizing enterocolitis (NEC), a life-threatening condition characterized by inflammation and death of intestinal tissue. FDA first learned of adverse events possibly linked to the product May 13, 2011. To date, the agency is aware of 15 cases of NEC, including 2 deaths, involving premature infants who were fed SimplyThick for varying amounts of time. Source: http://www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm256257.htm

Early test results show no E. coli in suspect German sprouts. No traces of the deadly E. coli bacteria have been found in initial tests at a German bean sprout farm suspected of being the source of the outbreak that has killed at least 22 people, agriculture officials in the state of Lower Saxony said June 6. But authorities said they might not find any evidence of E. coli if it affected only a batch of bad sprouts, and it is no longer in the supply chain. Test results are back for 20 of the 40 samples. It was not clear when the rest of the test results would be available. Officials June 5 said German-grown sprouts were the likely source for the outbreak. The agricultural minister in Lower Saxony said there is a “direct link” between a company in the town of Bienenbuettel and “these people getting sick.” The firm has been shut down, and its products have been recalled. The outbreak of a virulent strain of E. coli has infected more than 2,200 people in 12 countries, European health authorities said June 5. Germany said Spanish produce was not the source of the infection, and Spanish farmers are demanding hundreds of millions of euros in compensation from Germany. Two women and a man who traveled in May to northern Germany remain hospitalized in the United States with hemolytic uremic syndrome (HUS) — a form of kidney failure a U.S. Centers for Disease Control and Prevention spokesman said June 3. A fourth person developed bloody diarrhea, but was not hospitalized, he added. Two U.S. service members in Germany also developed diarrhea. Source: http://www.cnn.com/2011/WORLD/europe/06/06/europe.e.coli/index.html?hpt=hp_t2

Government Sector (including Schools and Universities)

(Georgia) **2 charged in copper thefts at Sugar Hill Elementary.** A 21-year-old man and a teenage juvenile were charged June 7 in connection with copper thefts at Sugar Hill Elementary School in Hall County, Georgia. The school was burglarized overnight June 6, with 11 heating, ventilation, and air conditioning units damaged. Copper tubing was torn from the large rooftop units, causing between $75,000 and $100,000 in damage, the Hall County Sheriff's Office chief deputy said. The suspects were charged with felony theft by taking, felony criminal damage, and possession of tools of a crime. A patrol officer noticed an open gate leading to the school at 1:28 a.m. June 7, but investigators said they think the perpetrators had already left the scene. When the damage was discovered around 9:30 a.m. June 7, the school system offered a $5,000 reward for information leading to an arrest. The suspects were charged within 24 hours of the reported damage. This is the second time in 2011 that copper wiring has been stolen from the school's air conditioning units. Source: http://www.gainesvilletimes.com/section/6/article/51509/

(Illinois) **Hazmat scare at federal building in Loop.** Chicago, Illinois police and fire officials investigated a report of a suspicious package possibly containing "bio hazard" contents at a Loop federal building, officials said. Police and fire officials were called at about 10:30 a.m. June 7 to 77 W. Jackson Boulevard after a package was delivered to a mailroom in the building, listed as the Ralph H. Metcalfe Federal Building, which houses a Social Security office. Fire officials said they are treating the incident as a hazardous materials incident, a spokesman indicated. Police said the package was sent to the building with the words "bio hazard" written on it. No injuries or evacuations were reported. Source: http://www.chicagotribune.com/news/local/breaking/chibrknews-haz-mat-response-called-for-federal-building-in-the-loop-20110607,0,2347025.story?track=rss

Information Technology and Telecommunications

Plankton Android trojan found in 10 apps on Android Market. Ten more applications have been pulled from Google's official Android Market following a notification that they contained a new kind of Android malware. The malware was discovered by an assistant professor at the North Carolina State University and his team. The malicious code is "grafted" onto legitimate applications, and once the app is installed, it works as a background service whose goals is to gather information and transmit it to a remote server. The server takes the information in consideration and returns a URL from which the malware downloads a (dot)jar file that, once loaded, exploits Dalvik class loading capability to stay hidden by evading static analysis. According to the researchers, Plankton — as they named the malware — and the payloads it downloads do not provide root exploits. "Instead, they only support a number of basic bot-related commands that can be remotely invoked," they said. Among those commands are those that collect browser history, bookmark and log information, and those that allow the

installation and deinstallation of shortcuts. Source: http://www.net-security.org/malware_news.php?id=1745

New malware can launch multiple types of advertising fraud. A new coordinated malware attack can enable cybercriminals to launch multiple types of online advertising fraud, according to researchers. According to researchers at Adometry (formerly Click Forensics), the attack, called "ad hijacking," uses similar malware and infection delivery methods to create a network of computers aimed at committing advertising fraud through different kinds advertisements and channels. "In the past, advertising fraudsters have mainly set their sights on the search advertising industry," the CEO of Adometry said. "This is the first attack we've seen that coordinates advertising fraud across many different online ad channels." Rather than requiring a user to download malware via a fake antivirus program, Adometry said the ad-hijacking malware injects itself into the rootkit of a user's computer through an advertisement on a popular Web site. Once it infects the computer, the malware receives instructions from a host to perform multiple kinds of advertising fraud, including search hijacking, display advertising impression inflation, and video advertising fraud. Source: http://www.darkreading.com/security/vulnerabilities/230200004/new-malware-can-launch-multiple-types-of-advertising-fraud.html

Java 6 update 26 fixes critical security issues. Oracle has released update 26 for its Java SE 6 platform to address a number of 17 remotely exploitable vulnerabilities, many of which could result in arbitrary code execution. Of the included patches, 11 apply only to the Java SE client and 1 only to the server version. The rest affect both of the platform's flavors. Nine vulnerabilities carry the maximum score of 10 on the CVSS scale. This means that they can be exploited remotely with ease and no authentication resulting in a complete confidentiality, integrity, and availability compromise. The scores were calculated under the presumption users have administrative privileges, typically on Windows, and are capable of running Java applets or Java Web Start applications that is default behavior. Three of the remaining vulnerabilities carry a CVSS base score of 7.6, four of 5.0, and one of 2.6. Java vulnerabilities are commonly exploited in drive-by download attacks to infect users with malware. In fact, according to statistics grabbed from live Web exploit kit installations, Java exploits are the most effective ones. Source: http://news.softpedia.com/news/Java-6-Update-26-Fixes-Critical-Security-Issues-204840.shtml

Android app brings cookie stealing to unwashed masses. A developer has released an app for Android handsets that brings Web site credential stealing over smartphones into the script kiddie realm. FaceNiff, as the Android app is called, can be used to steal unencrypted cookies on most Wi-Fi networks, giving users a point-and-click interface for stealing sensitive authentication tokens sent over Facebook, Twitter, and other popular Web sites when users do not bother to use encrypted secure sockets layer (SSL) connections. The app works even on networks protected by WPA and WPA2 encryption schemes by using a technique known as ARP spoofing to redirect local traffic through the attacker's device. Source: http://www.theregister.co.uk/2011/06/03/android_cookie_stealing_app/

DroidKungFu malware discovered on Android platform. Computer researchers are warning Android users of another malware campaign targeted at the platform, which appears to circumnavigate traditional anti-virus filters. North Carolina State University researchers identified at least two applications in more than eight third-party app stores and forums based in China infected with the DroidKungFu malware. The malware mainly affects Android 2.2, exploiting two vulnerabilities to install a back door on a victim's device which allows hackers to take complete control, according to a post on the university's official blog. "Previously identified malware, such as DroidDream, has also taken advantage of these two vulnerabilities. But [the researchers] think DroidKungFu is different because, based on the early results of their research, it does a better job of avoiding detection by security software," the blog noted. "And, while later versions of Android have patched these vulnerabilities, they are not entirely secure. The security patches severely limit DroidKungFu, but it is still able to collect some user data — such as a mobile phone device ID number — and send them to a remote site." Source: http://www.v3.co.uk/v3-uk/news/2076365/droidkungfu-malware-discovered-android-platform

After hack, RSA offers to replace SecureID tokens. In an acknowledgment of the severity of its recent computer compromise, RSA Security said June 6 that it will replace SecureID tokens for any customer that asks. Customers have been left wondering whether to trust RSA's security tokens since March, when the company acknowledged it had been hacked and issued a vague warning to its customers. Then, 2 weeks ago, government contractor Lockheed Martin was reportedly forced to pull access to its virtual private network after hackers compromised the SecureID technology. In a letter sent to customers June 6, RSA confirmed the Lockheed Martin incident was related to SecureID. Information "taken from RSA in March had been used as an element of an attempted broader attack on Lockheed Martin," RSA's executive chairman said in the letter. He said the company remains "highly confident in the RSA SecureID product," but noted the recent Lockheed Martin attack and general concerns over hacking, "may reduce some customers' overall risk tolerance." Source: http://www.computerworld.com/s/article/9217381/After_hack_RSA_offers_to_replace_SecureID_tokens

Nintendo says U.S. server breached, no data lost. Nintendo was targeted in a recent online data attack, but no personal or company information was lost, the Japanese company said June 5. The server of an affiliate of Nintendo Co.'s U.S. unit was accessed unlawfully a few weeks ago, but there was no damage, according to a company spokesman. "There were no third-party victims," he said, "but it is a fact there was some kind of possible hacking attack." Lulz Security claimed credit for the Nintendo attack, posting what they said was a Nintendo server configuration file to the Web. Source: http://www.msnbc.msn.com/id/43283396/ns/technology_and_science-security/

Adobe ships emergency fix for Flash bug. Adobe has released an out-of-cycle update for Flash that fixes a serious vulnerability in the application on all platforms. The bug is a cross-site scripting flaw that can be used in drive-by download attacks and Adobe said it is currently being used in some targeted attacks. Adobe security officials said they first found out about the Flash vulnerability June 3, and the company was able to develop and release a fix for it June 5. The

bug exists in Flash running on Windows, Mac OS X, Android, Linux, and Solaris. "An important vulnerability has been identified in Adobe Flash Player 10.3.181.16 and earlier versions for Windows, Macintosh, Linux and Solaris, and Adobe Flash Player 10.3.185.22 and earlier versions for Android. This universal cross-site scripting vulnerability (CVE-2011-2107) could be used to take actions on a user's behalf on any website or webmail provider, if the user visits a malicious website. There are reports that this vulnerability is being exploited in the wild in active targeted attacks designed to trick the user into clicking on a malicious link delivered in an email message," Adobe said in its advisory. Source: http://threatpost.com/en_us/blogs/adobe-ships-emergency-fix-flash-bug-060611

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

(Nebraska) **Police secure post office after bomb threat.** Police secured the U.S. Post Office at Nebraska City, Nebraska, after receiving a report of a bomb threat at 3:56 p.m. June 3. Police made sure everyone was out of the building, including two post office employees, and taped off the Central Avenue parking spaces and parking lot. A Nebraska State Patrol dog was brought into the inspect the building. The dog indicated on two packages, but they were not a threat. Postal investigators are working to track the source of the threat. Police re-opened the drive through lanes for postal customers by 7:30 p.m. Source: http://www.ncnewspress.com/news/x437334368/Police-secure-post-office-after-bomb-threat

(Iowa) **Five Iowa post offices to evacuate.** Five southwest Iowa post offices threatened by floodwaters have been evacuated. The U.S. Postal Service made the announcement June 3. On June 4, operations at the Modale, Iowa, office moved to Missouri Valley. The Blencoe, Iowa, post office moved to the Moorhead, Iowa, post office. The Percival, Iowa, post office moved to the Sidney, Iowa, post office. On June 7, the Hamburg, Iowa, post office will move to the Sidney, Iowa, post office. Operations at the Pacific Junction, Iowa, post office will move to the Glenwood, Iowa, post office. Officials said customers served by the affected post offices should pick up their mail at the new locations. Letter carriers will continue to deliver to businesses and residences where possible. The moves are in effect until further notice. Source: http://www.ketv.com/r/28121331/detail.html

Public Health

Vygon recalls hospital kits over wipes. Medical device company Vygon recalled some hospital-use convenience kits because they contain Skin-Prep Wipes that were subjected to a prior

recall. Vygon said the week of May 30 its Churchill Medical Systems company was starting a recall of certain lots of wipes, mostly dressing change kits. The wipes were affected by an April recall due to the potential for bacterial contamination. Vygon said no contamination has been found and no injuries have been reported, but the company started the recall because contaminated wipes can lead to life-threatening infections. The kits were shipped to distributors and hospitals between September 3, 2010, and March 11, 2011. Source: http://www.businessweek.com/ap/financialnews/D9NMK7900.htm

FDA steps in to prevent drug shortages. The Food and Drug Administration (FDA) was able to prevent 38 "close calls" from turning into drug shortages in 2010 by speeding approval of manufacturing changes or forewarning drugmakers, FiercePharma Manufacturing reported June 7. It also facilitated the import of drugs not approved for use in the United States to maintain supplies of medically necessary treatments. An FDA spokeswoman said the agency helped some manufacturers address quality and manufacturing issues so "supplies could continue to be available while ensuring no risk for U.S. patients." In addition, the agency approved new manufacturing sites, as well as raw material and component suppliers in time to avoid a shortage, thanks to early notification from drugmakers. When notified in advance by drugmakers that intended to discontinue multi-sourced drugs, regulators informed other suppliers so they could be ready to meet the shortfall. In April, the FDA worked with cytarabine-producers Hospira, APP Pharmaceuticals, and Bedford Labs during an API shortage. It located an overseas maker of the leukemia drug willing to temporarily import the injections for U.S. use, even though the import is technically unapproved by the regulator. Another case involves the anticancer drug, Fusilev (levoleucovorin, in 50-mg single-use vials) from Spectrum. In this case, the regulator gave the drugmaker temporary permission to import levoleucovorin 100-mg powder for injection for U.S. distribution. Source: http://www.fiercepharmamanufacturing.com/story/fda-steps-prevent-drug-shortages/2011-06-07

TRANSPORTATION

Amtrak services disrupted in Neb., Iowa and Colo. Flooding along the Missouri River in the Omaha, Nebraska area is forcing Amtrak to disrupt its California Zephyr passenger train, which travels between San Francisco, California, and Chicago, Illinois. Amtrak said June 7 that service will be temporarily suspended between Denver, Colorado, and Chicago for at least 6 days because of predicted flood crests and additional closures of Burlington Northern Santa Fe tracks in the Omaha area. Amtrak said in a statement the suspension of service is effective with an eastbound train June 9 from Emeryville, California, and a westbound train June 10 from Chicago. The disruption is expected to continue through at least June 14. Source: http://www.beaumontenterprise.com/news/article/Amtrak-services-disrupted-in-Neb-Iowa-and-Colo-1413852.php

Water and Dams

(Iowa; Missouri; Nebraska) **Army expects full breach of Missouri River levee.** Crews scrambled June 6 to protect a southwest Iowa town from the swollen Missouri River, but Hamburg officials said it is unclear whether they will be able to prevent the river from leaving the community under several feet of water for weeks. If efforts to pile massive sandbags on a faltering levee and build a secondary barrier fail, part of Hamburg could be under as much as 8 feet of water for a month or more, a fire chief said. Flooding along the river this summer — expected to break decades-old records — will test the system of levees, dams and flood walls like never before. The earthen levee that guards an area of farmland and small towns between Omaha, Nebraska, and Kansas City, Missouri has been partially breached in at least two places south of the Iowa-Missouri border. Emergency management officials expect new breaches in the coming days as the river rises. The last time the Missouri River crested at levels predicted for this summer happened in 1952, before most of the major dams along the river were built. The flooding is expected to last into mid-August. The U.S. Army Corps of Engineers will be releasing more water than it ever has from the dams by mid-June, meaning there likely will be other levee problems like the ones near Hamburg, said an official with the Corps' water management office. Officials also predict that the water will get high enough to flow over at least 11 levees in the area near Hamburg in the corners of southeast Nebraska, southwest Iowa, and northwest Missouri. Source: http://www.foxnews.com/us/2011/06/06/missouri-river-levee-springs-2nd-partial-breach/

(Wyoming) **Thousands of gallons of oil likely leaked in creek.** Federal officials said malfunctioning equipment on an oil well led to a leak of as many as 10,000 gallons into a creek south of Rawlins, Wyoming. The U.S. Environmental Protection Agency (EPA) said the spill into Emigrant Creek ranged between 1,000 and 10,000 gallons but it is likely closer to the upper total. The Casper Star-Tribune reported the EPA is leading the cleanup of the southern Wyoming site, in coordination with the Bureau of Land Management and the Wyoming Department of Environmental Quality. Authorities said they learned of the oil spill May 22, but believe it occurred "some time ago." They are reviewing possible consequences for the owner of the well, Denver-based Nadel and Gussman Rockies. Officials said no oil has been found downstream in Little Sage Creek or Teton Reservoir. Source: http://www.kulr8.com/news/wyoming/123289603.html

(Iowa; Missouri) **Missouri levee breach prompts evacuations in Iowa.** About 600 residents in southwest Iowa were ordered June 5 to evacuate their homes after the Missouri River breached a levee across the border in Missouri. The evacuation covers nearly half of the town of Hamburg, a spokeswoman for the Iowa Department of Homeland Security and Emergency Management (IDHSEM) said. Residents, most of them on the south side of the city of 1,141, were told to get out within 24 hours. The U.S. Army Corps of Engineers reported a levee was breached June 5 south of Hamburg in Missouri's Atchison County. A Corps spokesman said crews had been working June 4 on another issue near the breach and all workers were evacuated. The IDHSEM head characterized the breach as a "boil" — a leak that "shoots out like a small geyser" — that was 1 inch to 1.5 inches in diameter. Iowa sent a Blackhawk helicopter

June 5 to drop roughly 1,000-pound sandbags on the levee, he said, adding it was too dangerous to use ground crews. It was not known how long the work would take. The emergency management director for Atchison County, Missouri, said another nearby levee had a similar break June 4, but she said crews were able to repair it. She said levees along the Missouri River have been weakened by the river's recent high water levels. Source: http://www.ctpost.com/news/article/Missouri-levee-breach-prompts-evacuations-in-Iowa-1410544.php

(New York) **'Unacceptable' level of sewage bacteria in river, creek.** Recent testing of water from the Hudson River and Catskill Creek in Greene County, New York by the advocacy organization Riverkeeper has discovered the presence of an "unacceptable" level of sewage bacteria. Enterococcus, a bacteria normally found in human feces, was found in amounts exceeding U.S. Environmental Protection Agency limits in 80 percent of samples taken from New York City to Saratoga County May 19. Eight samples between Catskill and Coxsackie, including at the Hudson boat launch, exceeded, in some cases by as much as 10 times, the permitted Enterococcus count of 61 per 100 milliliters. Source: http://www.thedailymail.net/articles/2011/06/06/news/doc4dec0960e94a3819087312.txt

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168